WHAT IS CLAIMED IS:

1. In a system coupled between a protection network and an external network, for detecting intrusion states between the protection and external networks and preventing the intrusion, an in-line mode network intrusion detecting and preventing system comprising:

a first network processor unit for monitoring an externally received PDU (packet data unit), collecting various statistical data according to a metering rule, selectively discarding or passing the received PDU according to a packet preventing rule, and generating a duplicate of the PDU according to a sensing rule;

a second network processor unit for applying at least one attack signature to a payload of the PDU received from the first network processor unit, and detecting intrusion states between the protection and external networks; and

a personal computer for generating or updating a packet preventing rule for preventing the intrusion detected by the second network processor unit, and providing the packet preventing rule to the first network processor unit.

2. The system of claim 1, further comprising a line interface for transmitting at least one PDU received from an external Ethernet interface to the first network processor unit.

3. The system of claim 2, wherein the personal computer generates or updates a packet preventing rule and a sensing rule which include at least one of a transmitter port address and a destination port address of the PDU, a transmitter IP (Internet protocol) address, a destination IP address, a protocol,

and a TCP (transmission control protocol) flag bit or which include a combination of at least two of them.

4. The system of claim 3, wherein the personal computer generates or updates a metering rule which includes at least one of a transmitter Ethernet address, a destination Ethernet address, and an Ethernet type of the PDU, a transmitter IP address, a destination IP address, a transmitter port address, a destination port address, a protocol, and a TCP flag bit or which includes combinations of at least two of them.

5. The system of claim 4, wherein the first network processor unit comprises:

a sorter for determining whether to discard or pass the PDU received from the line interface according to the packet preventing rule received from the personal computer, and determining whether to duplicate the received PDU according to the sensing rule received from the personal computer;

a traffic manager for discarding the received PDU or duplicating the PDU determined to be sensed thereby generating a duplicate of the PDU, according to a discarding determination by the sorter; and

a state engine for managing various statistical data relating to the PDU received from the line interface, according to the traffic metering rule received from the personal computer.

6. The system of claim 5, wherein the first network processor unit further comprises:

first to fourth logic ports for outputting the PDU to the Ethernet interface, or receiving the PDU from the Ethernet interface;

a link layer receiver for receiving the duplicate of the PDU from the state engine;

a PDU converter/duplicator for generating a BPDU (bearer PDU) and an SPDU (shortened PDU) by using the received duplicate of the PDU; and

a PHY transmitter for transmitting the generated BPDU and the SPDU to the second network processor unit.

7. The system of claim 6, wherein the second network processor unit comprises:

a sorter for performing pattern matching on the payloads of the transmitted BPDU and the SPDU according to the rule received from the personal computer, and detecting the intrusion state between the protection and external networks;

a state engine for collecting and managing information on the detected intrusion state; and

a PCI interface for transmitting the collected and managed information to the personal computer.

8. In a method for detecting intrusion states between a protection network and an external network, and preventing the intrusion, an in-line mode network intrusion detecting and preventing method comprising:

(a) generating a packet preventing rule which is a reference for discarding at least one externally received PDU (packet data unit) or passing the same;

(b) selectively discarding or passing the received PDU according to the generated packet preventing rule;

(c) applying at least one attack signature to a payload of the passed PDU, and detecting the intrusion state between the protection and external networks; and

(d) generating or updating a rule for preventing the detected attack, and preventing the detected attack.

9. The method of claim 8, wherein (a) comprises:

generating or updating a packet preventing rule which includes at least one of a transmitter port address and a destination port address of the received PDU, a transmitter IP (Internet protocol) address, a destination IP address, a protocol, and a TCP (transmission control protocol) flag bit or which includes combinations of at least two of them;

generating or updating a sensing rule which includes at least one of a transmitter port address and a destination port address of the received PDU, a transmitter IP (Internet protocol) address, a destination IP address, a protocol, and a TCP (transmission control protocol) flag bit or which includes combinations of at least two of them; and

generating or updating a metering rule which includes at least one of a transmitter Ethernet address, a destination Ethernet address, and an Ethernet type of the received PDU, a transmitter IP address, a destination IP address, a transmitter port address, a destination port address, a protocol, and a TCP flag bit or which includes combinations of at least two of them.

10. The method of claim 9, wherein (b) comprises:

determining whether to discard or pass the externally received PDU according to the generated or updated packet preventing rule;

discarding the received PDU when it is determined to discard at least one PDU from among the received PDUs;

duplicating the PDU to be passed and generating a duplicate of the PDU when it is determined to pass at least one PDU from among the received PDUs; and

adding an ID to the duplicate of the PDU, and outputting the ID-added duplicate of the PDU, the ID being addition information.

11. The method of claim 10, wherein (b) further comprises:

generating a BPDU (bearer PDU) by using the duplicate of the PDU; and

generating an SPDU (shortened PDU) having a size less than that of the generated BPDU, and outputting the SPDU and the BPDU.

12. The method of claim 11, wherein (c) further comprises:

performing pattern matching to compare payloads of the BPDU and the SPDU with the attack signature provided by a manager for managing the protection or external network; and

detecting the attack states to the protection or external network according to a performed pattern matching result, transmitting the detection result to the manager, and updating or generating the attack signature provided by the manager.